International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471
Vol. 2 Issue 9, Nov.-Dec., 2013, pp: (36-39), Available online at: www.erpublications.com

Avant-garde Security in AODV

Ms. Sonika Malik, Sahil Kapoor, Chirag Chopra,
Vivek Mishra, Rashmi Chaudhary
Department of IT, MSIT, New Delhi, India

Abstract: MANETs are networks formed by moving nodes. They use wireless communication to speak among them and they do it in an ad hoc manner. MANET is considered as an ideal network model for group communications because of its forte of instant establishment. Since, existence of central servers cannot be expected; nodes need to guarantee their data to reach the destination securely without loss, tamper or theft of information. This paper explains and compares two ways to ensure data is securely reached to destination. First approach (iAODV) is designed for MANET where symmetric keys can be made available at time of set up of network. It uses intelligent detection and avoidance of probable malicious nodes occurring in route path by scanning packet tampering. Second approach (fAODV) is designed to deliver the encryption keys through 'friend' nodes before sending data packets. The results prove that the whole MANET structure can be upheld at a reasonable security level with practical short convergence time on small computation expenses. More importantly, the security level can be easily customized to meet the varied demands from applications over ad hoc networks.

Keywords: AODV, MANET, Security, iAODV, fAODV, Super Secure channel.

I. INTRODUCTION

MANET is anassembly of self-governing mobile users that communicate over relative bandwidth and power constrained wireless links. MANET has know-how to establish networks at anytime, anywhere. These networks are fabricated, work and sustainedon its own because each node accomplishes dual role of host and router. In general, these nodes have a narrow transmission range and so each node search for the backing of its neighboring nodes in sending packets. This exclusive feature is responsible to route the packetregardless ofchanging topology of network.

AODV is a distance vector routing protocol that has been logically build for MANETs. AODV is reactive(on demand) in nature as it looking for the routes only when necessary. To dodge the problem of generation of outing loops, it makes extensive use of sequence-numbers in control packets. When a source node is concerned to connect with a destination node whose route is not known, it broadcasts a Route Request (RREQ) packet. Each RREQ packet has a Request ID, hop count, flags,source and destination node IP addresses and sequence numbers. The Request ID field exclusivelyrecognizes the RREQ packet; the sequence numbers gives factsabout the newness of control packets and the hop-count keeps the number of nodes between the source and the destination. Receiver node of the RREQ packet that has not discovered the Source IP and ID pair or doesn't keep a fresher (larger sequence number) route to the destination rebroadcasts the same packet after increasing the hop tally. Such intermediary nodes also create and save a REVERSE ROUTE to the source node for a sometime. When the RREQ packet reaches at the destination node or any intermediary node that has a newer route to the destination a Route Reply (RREP) packet is created and directed back to the source.

RREP packet has the destination node sequence number, the source and the destination IP addresses, route lifespan, hop tally and flags. Intermediate node that obtains the RREP packet, increases the hop count, establishes a Forward Route to the source of the packet and conveys the packet on the Reverse Route. When a link failure is detected for a next hop of an active route a Route Error (RERR) message is sent to its active neighbors that were using that specific route.

These networks don't depend on superfluous hardware which makes them an idyllic candidate for military services and tasks. For example, battle field ad hoc network, in such a network we would surely be first worried with the efficient and in time transfer of the message but with this, we will have to be more worried about the strong secrecy of the information also.AODV doesn't offer any safety for data it is sending. This is major disadvantage in AODV which has been addressed and countered in various researches.

Our paper also uses two techniques, one implemented for MANETs where symmetric keys can be provided and other where asymmetric keys are used.

II. PROPOSED SYSTEMS

a) iAODV

(i) Introduction

We concern the security problem introduced by the unsteadiness of physical laye. AODV is susceptible to various kinds of attacks. There are two main stimuli which encourage nodes to misbehave: self-centeredness and malice. When dealing with packet-forwarding, there are several kinds of availability and integrity attacks: dropping (complete or partial), misrouting, modification and fabrication. Malicious cooperation (such as a wormhole attack) and identity changes are also challenges attacks.

We assume that MANET used is supplied with symmetric key pairs to all nodes i.e. each pair of nodes has unique combination of key with other nodes. These secret keys are used to encrypt and decrypt data. We design a new simple algorithm to generate link error at the point of detection of unviable or corrupt packets at the destination node which breaks the current route. Though this causes excessive overload in network, the packet information is secured and fabrication is prevented.

ii) Initialization

The nodes in network are initialised with empty routing tables. Every node is provided with a Unique ID (IP Address). The network distributes UNIQUE KEY pairs for encryption and decryption of messages to all nodes. For N nodes, total key pairs are n*(n-1). No two nodes know the *secret key pair* of any other node pair. Every node has an encoding key for each node in network which it uses to encode the data packet and decoding key for each node which is used to decode the data.

iii) NCI index (Non Credibility Index is) stored in trust table. It is updated whenever a packet is received. If Packet is corrupted it increases the NCI value of nodes in route path, depicting probable malicious nodes. If the packet is received successfully, then the good behavior of nodes is path is rewarded with decrease in the NCI index. NCI index is only increased at the destination end.

iii) Working

The data packet is encrypted using symmetric key encrypting algorithm using the secret pair of keys between source and destination node. Then the message goes under RSA encryption and signature is generated. The public key and digital signature are sent along with the packet (can be secured via hash chain). Destination node maintains a special table; let us call it trust-table, of all nodes in network. This trust-table is supposed to store non-credibility-index (NCI) along with IP address of possible malicious nodes. Whenever destination receives a tampered packet (which is detected by the RSA algorithm using public signature and key provided as shown in SAODV in previous chapter), it increases NCI Value of all nodes in route path, depicting one or more than one nodes in the path is malicious. If the packet is delivered with successful signature verification, the NCI Value of all nodes in route path is decreased. This ensures that no ‘good’ node is getting killed in network because it appears too frequently in bad paths. It acts like Artificial Intelligence to filter good and bad nodes through the trust table it forms during course of time. There is a threshold value set for NCI value for nodes, after which the nodes will be avoided in setting up path. The NCI index, if higher than threshold value for more than half nodes in the network is normalized by reducing values to lower levels to avoid rejection of too many paths. This ensures that network is always up and running.

b) *f-AODV*

i) Introduction

The main problem in distributing secret keys is that they must be connected to each other or some common server at least once. This is not feasible in cases where few nodes may or may not be present be at the time of feeding of keys to nodes. Further if database of keys is leaked, the entire security structure entire would collapse. Or if the encryption/decryption algorithm is cracked, it would be easy to crack the message using brute force attack. To avoid these problems, we can deliver keys dynamically from Source to Destination through a ‘super secure’ channel before the data packet is sent. fAODV is solution for such kind of needs when we have information about our ‘friend’ nodes which may or may not be present at beginning of set up of MANET. When someone node wants to establish a connection, the path set up initially is through only these friend-nodes and the key for encryption/decryption of data packet sent are delivered through this ‘super secure’ channel only. The fAODV can use a bit of time in setting up the

super secure channel initially which is directly proportional to number of friend nodes in network for obvious reasons. This type of network can fail if the source gets isolated from other trusted nodes and is never able to set up the 'super secure' channel. It will not be able to send any packet.

ii) Working

When a source node is interested to communicate with a destination node whose route is unknown, it broadcasts a RREQ packet. The initial RREQ packets are extended with the private key and transpose matrix. The private key and transpose matrix are only sent until acknowledgement from destination is received. Until then, RREQ is advanced only through 'super secure' path. After that the whole system switches to normal AODV and sends packet to all in range legitimate nodes. Recipient node of the RREQ packet that has not find the Source IP and ID pair or doesn't maintain a newer larger sequence number route to the destination rebroadcasts the same packet after incrementing the hop-count. Any intermediate node that has a renewed route to the destination a RREP (Route Reply) packet is generated and sent back to the source.

c) *Result*

The following readings have been taken by building and simulating AODV protocol on a MANET in C++.
(N: Original AODV with no security, I: iAODV and T:fAODV)

1. Network Congestion

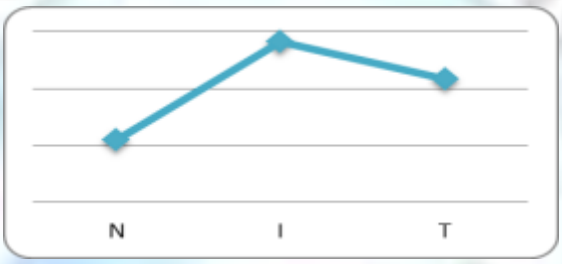

Figure 1: Network Congestion

i. AODV(Low): Since there is no security or path correction, the RREQ packets are very less.

ii. iAODV (High): Due to path rejection, the amount of RREQ packets increases as compared to fAODV or AODV, causing network congestion. Intelligent normalises the trust table to make sure not many nodes are facing rejections.

iii. fAODV (Low): The RREQ packets sent in TAODV are less than in beginning since they only travel through trusted nodes. Since there is no path rejection in TAODV, network congestion is very less than TAODV and SAODV.

2. Throughput (Packet received per Unit time)

i. AODV (High): The throughput of entire network is highest.
ii. iAODV (Higher): Very high throughput, if we ignore the loss of packets.
iii. fAODV (Average): Lower throughput because of time wasted in finding super secure path for delivering the key.

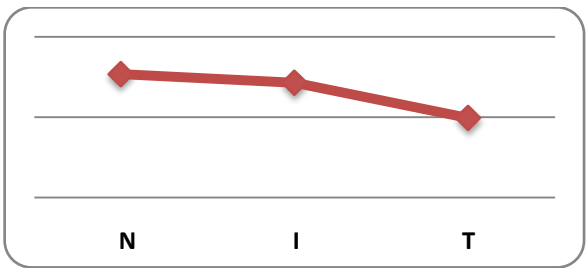

Figure 2: Throughput

3. *Delivery Ratio (Packets Successfully Received/ Packet Sent)*

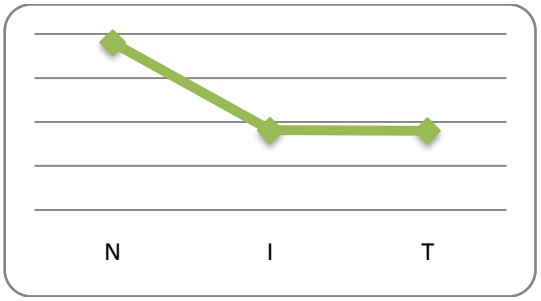

Figure 3: Delivery Ratio

i. AODV (High): The delivery ratio is very high but no security is implemented.

ii. iAODV (Average): Number of packets delivered is almost half than AODV but all packets delivered are safe and secure.

iii. fAODV (Average):Packet delivery ratio is slightly poorer than iAODV, but it requires no key distribution mechanism. Further considering the fact that time is wasted in setting up first time super secure channel, performance will be better for fAODV for large data.

III. Conclusion

iAODV caused lot of network congestion over basic AODV, but was able to avoid malicious paths. It also avoids impersonation of nodes because keys between different nodes are different and one cannot decrypt packet successfully unless correct key pair is known. It should be preferred in when probability of tampering is low.

fAODV was the betterwhen it comes to network congestion caused. The performance of fAODV increases proportionately with number of friend nodes in network. This protocol should be used when a high amount of confidential data is to be sent and friend nodes are high.

IV. Future Work

Our project is aimed at protecting only non-mutable fields. Various other security techniques like hash chain authentication can be implemented for mutable fields. For e.g., iAODV, there is a possibility that malicious nodes drops all the RREP generated from destination when malicious packet is identified. This causes source to believe it is still sending packets, though the link is broken. This can be avoided using hash chains and various other methods, which we will implement in next cycle.

Also, iAODV can be implemented to transform itself into fAODV after certain period of time based on the trust-table. The trust table can also be built by exchanging trust information between neighbor nodes, and thus making mutual trust based relationship to send packet.

V. References

[1]. C.E. Perkins, E. Belding-Royer, and S.R. Das, "Ad hoc On demand Distance Vector (AODV) routing," IETF RFC 3561, July 2003.
[2]. P. Papa dimitratos and Z. J. Haas, "Secure Routing for Mobile Ad-hoc Networks," in Proc. of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, TX, Jan. 2002.
[3]. Yuxia Lin, A. Hamed Mohsenian Rad, Vincent W.S. Wong, Joo-Han Song "Experimental Comparisons between SAODV and AODV Routing Protocols", WMuNeP'05, October 13.
[4]. N. Ch. Sriman Narayana Iyengar **,** "An Efficient And Secure Routing Protocol For Mobile Ad hoc Networks", 2010
[5]. David B. Johnson, David A. Maltz and Yih-Chun Hu. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks. Internet-Draft, draft-ietfmanet- dsr-10.txt, July 2004.
[6]. LoayAbusalah, Ashfaq Khokhar and Mohsen Guizani ," A Survey of Secure Mobile Ad Hoc Routing Protocols"2008.
[7]. Nidhi Sharma, (Student M.Tech.), R.M. Sharma, "Provisioning of Quality of Service in MANET"s performance Analysis & Comparison (AODV & DSR)", IEEE, 2010, V7-243.